CVE-2014-3882

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-3882
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-25 11:19:00 UTC
Updated	2014-06-25 14:35:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the Login rebuilder plugin before 1.2.0 for WordPress allows remote attac

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	12net	Login Rebuilder	1.0.0	All	All	All
Application	12net	Login Rebuilder	1.0.1	All	All	All
Application	12net	Login Rebuilder	1.0.2	All	All	All
Application	12net	Login Rebuilder	1.0.3	All	All	All
Application	12net	Login Rebuilder	1.1.0	All	All	All
Application	12net	Login Rebuilder	1.1.1	All	All	All
Application	12net	Login Rebuilder	1.1.2	All	All	All
Application	12net	Login Rebuilder	1.0.0	All	All	All
Application	12net	Login Rebuilder	1.0.1	All	All	All
Application	12net	Login Rebuilder	1.0.2	All	All	All
Application	12net	Login Rebuilder	1.0.3	All	All	All
Application	12net	Login Rebuilder	1.1.0	All	All	All
Application	12net	Login Rebuilder	1.1.1	All	All	All
Application	12net	Login Rebuilder	1.1.2	All	All	All
Application	12net	Login Rebuilder	All	All	All	All

References

Reference	Source	Link	Tags
JVN#05329568: Login rebuilder vulnerable to cross-site request forgery	JVN	jvn.jp	
【重要】WordPressプラグイン「Login rebuilder」におけるCSRFの脆弱性対策について « 12net.jp	CONFIRM	12net.jp	Patch, Ve
WordPress › Login rebuilder « WordPress Plugins	CONFIRM	wordpress.org	Patch
JVNDB-2014-000062	JVNDB	jvndb.jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.